

SC-900T00-A Module 3: Describe the Capabilities of Microsoft Security Solutions

Module Agenda


Describe basic security capabilities in Azure


Describe security management capabilities of Azure


Describe security capabilities of Azure Sentinel


Describe threat protection with Microsoft 365 Defender


Describe security management capabilities of Microsoft 365

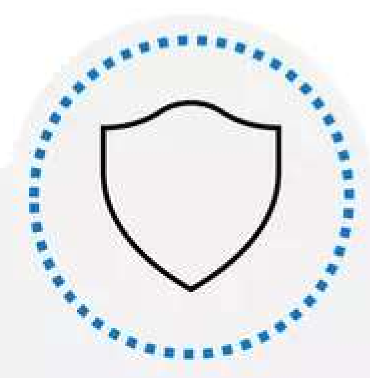

Describe endpoint security with Microsoft Intune

Lesson 1: Describe basic security capabilities in Azure

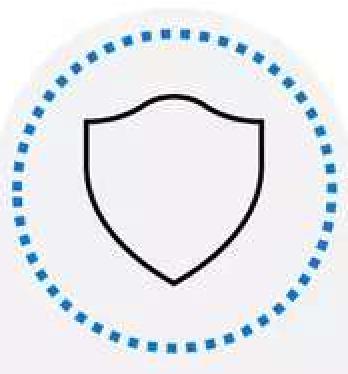


Lesson 1 Introduction

After completing this module, you should be able to:



Describe Azure security capabilities for protecting your network



Describe how Azure can protect your VMs

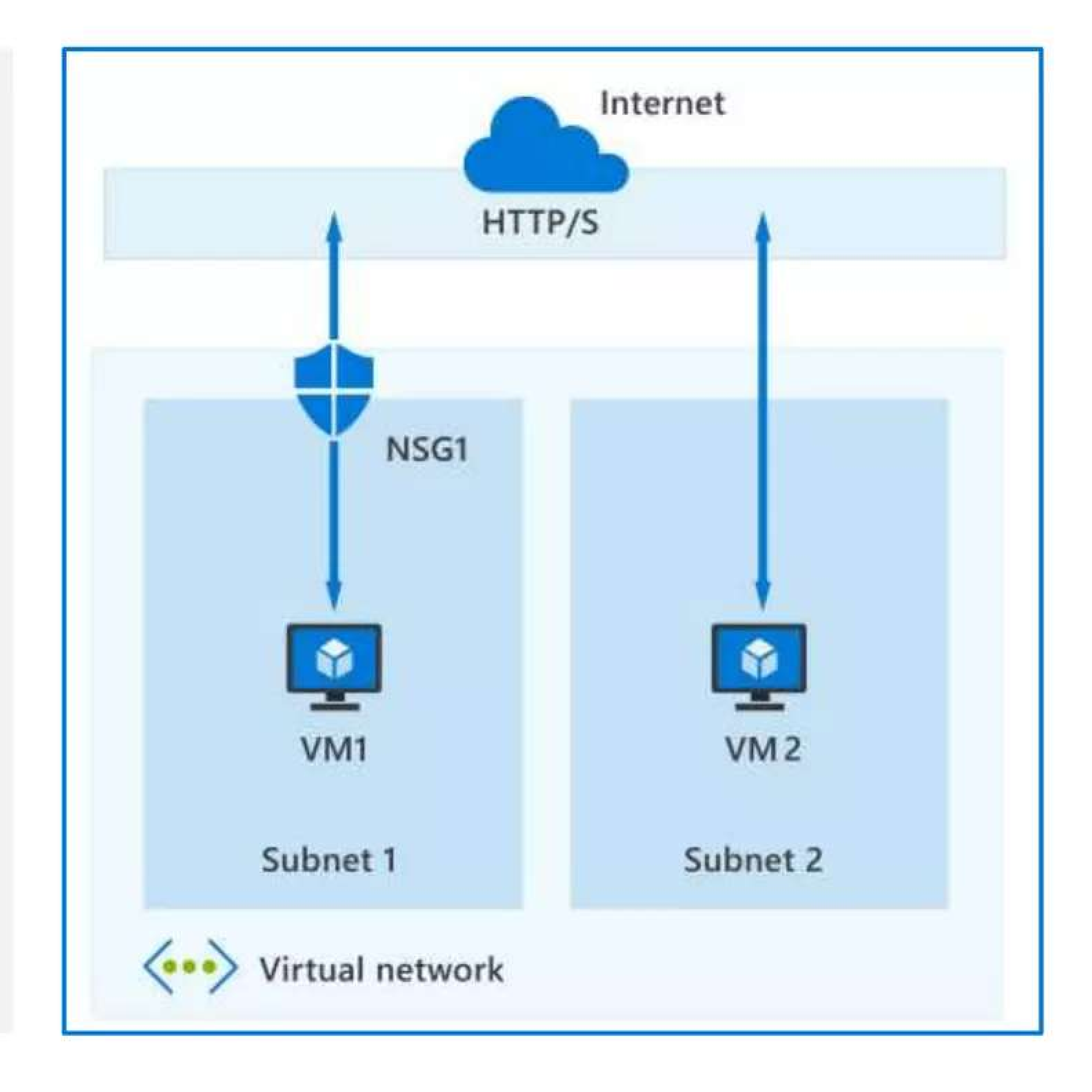


Describe how encryption on Azure can protect your data

Azure Network Security groups

Network security groups (NSG) let you allow or deny network traffic to and from Azure resources that exist in your Azure Virtual Network.

- An NSG can be associated with multiple subnets or network interfaces in a VNet.
- An NSG is made up of inbound and outbound security rules.
- Each rule specifies one or more of the following properties:
  - Name
  - Source or destination
  - Direction
  - Action
  - Priority
  - Protocol
  - Port range





Demo

Azure Network Security Groups

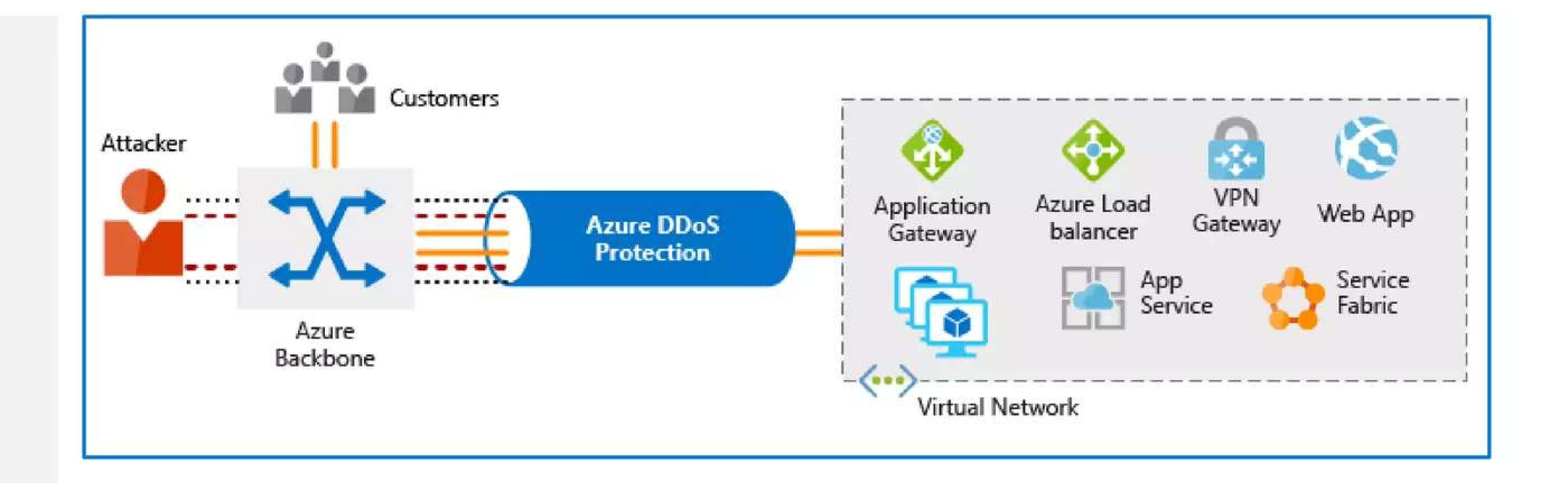
Azure DDoS protection

A Distributed Denial of Service (DDoS) attack makes resources unresponsive.

Azure DDoS Protection analyzes network traffic and discards anything that looks like a DDoS attack.

Azure DDoS Protection tiers:

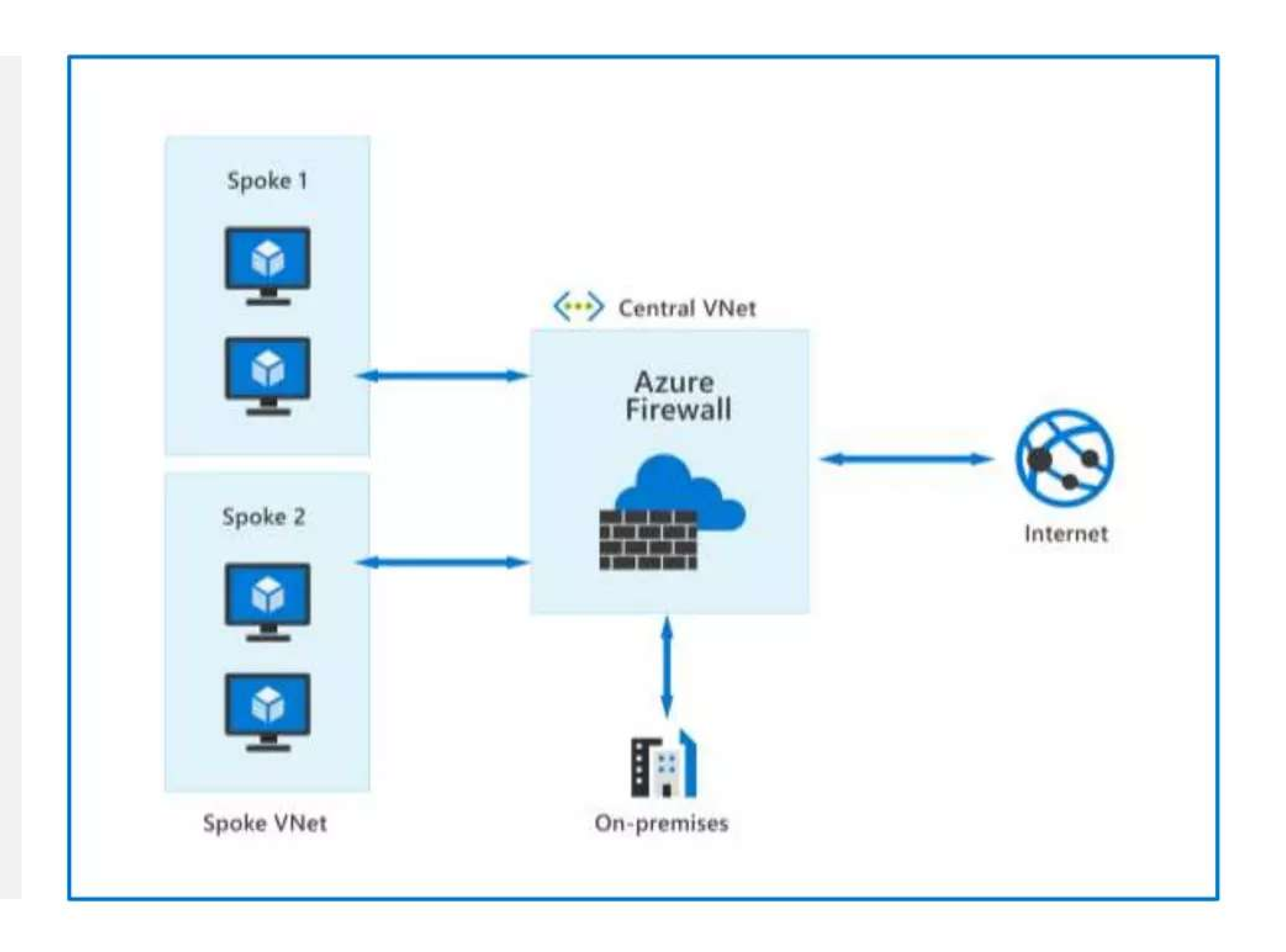
- Basic
- Standard



Azure Firewall

Azure Firewall protects your Azure Virtual Network (VNet) resources from attackers. Features include:

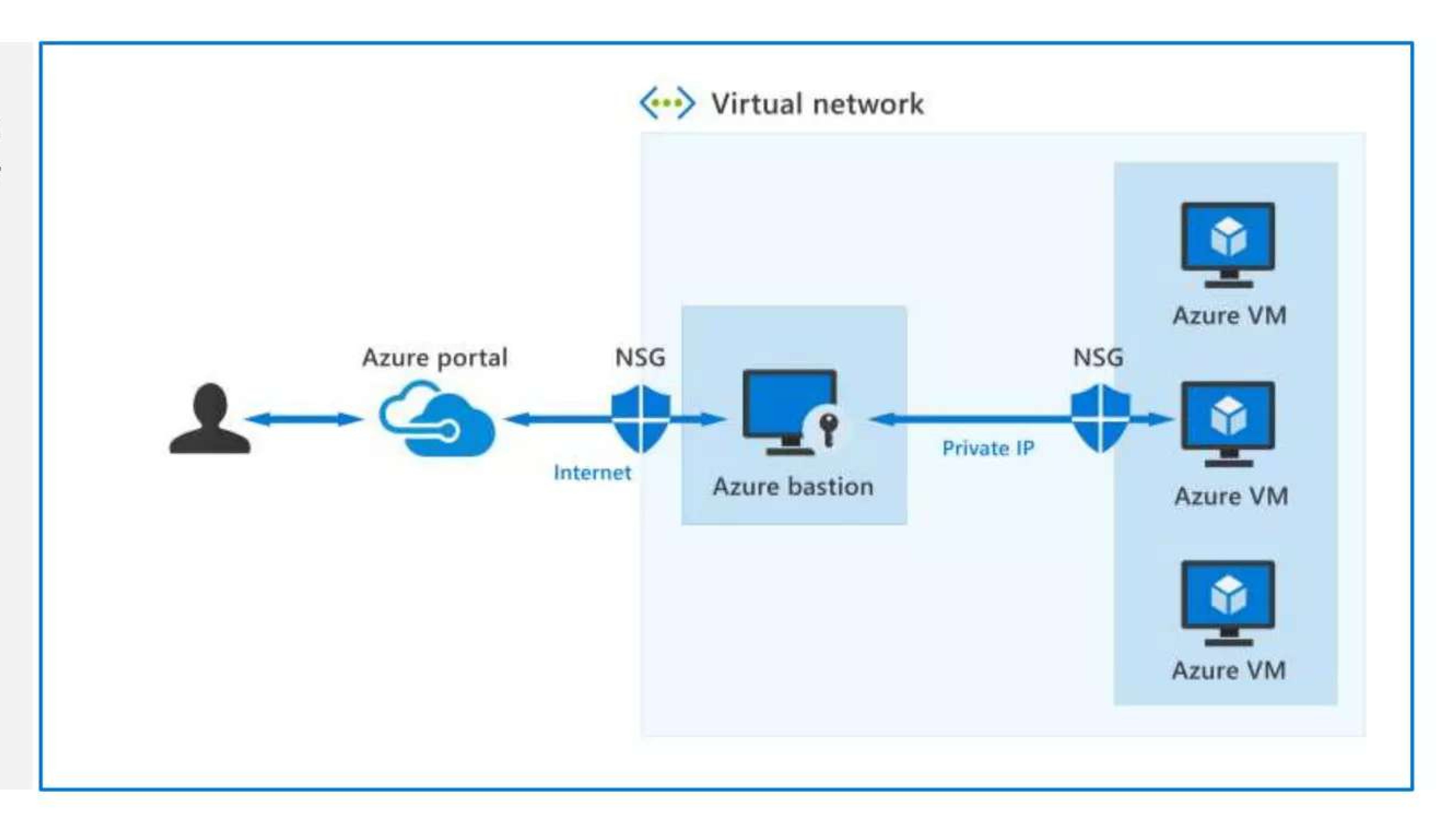
- Built-in high availability & Availability Zones
- Outbound SNAT & inbound DNAT
- Threat intelligence
- Network & application-level filtering
- Multiple public IP addresses
- Integration with Azure Monitor



Azure Bastion

Azure Bastion provides secure connectivity to your VMs directly from the Azure portal using Transport Layer Security (TLS). Features include:

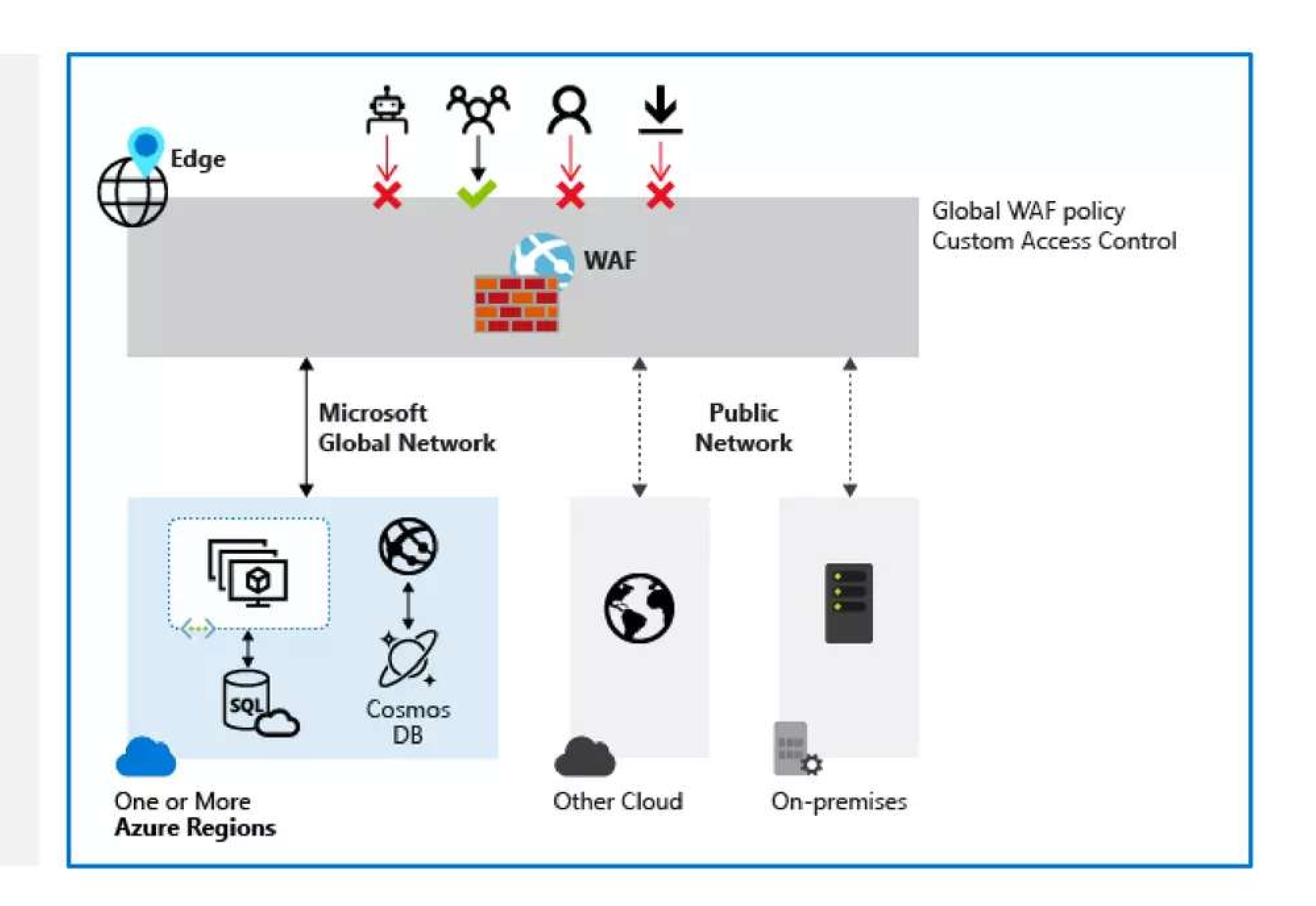
- RDP and SSH directly in Azure portal.
- Remote session over TLS and firewall traversal for RDP/SSH.
- No Public IP required on the Azure VM.
- No hassle of managing NSGs.
- Protection against port scanning.
- Protect against zero-day exploits.



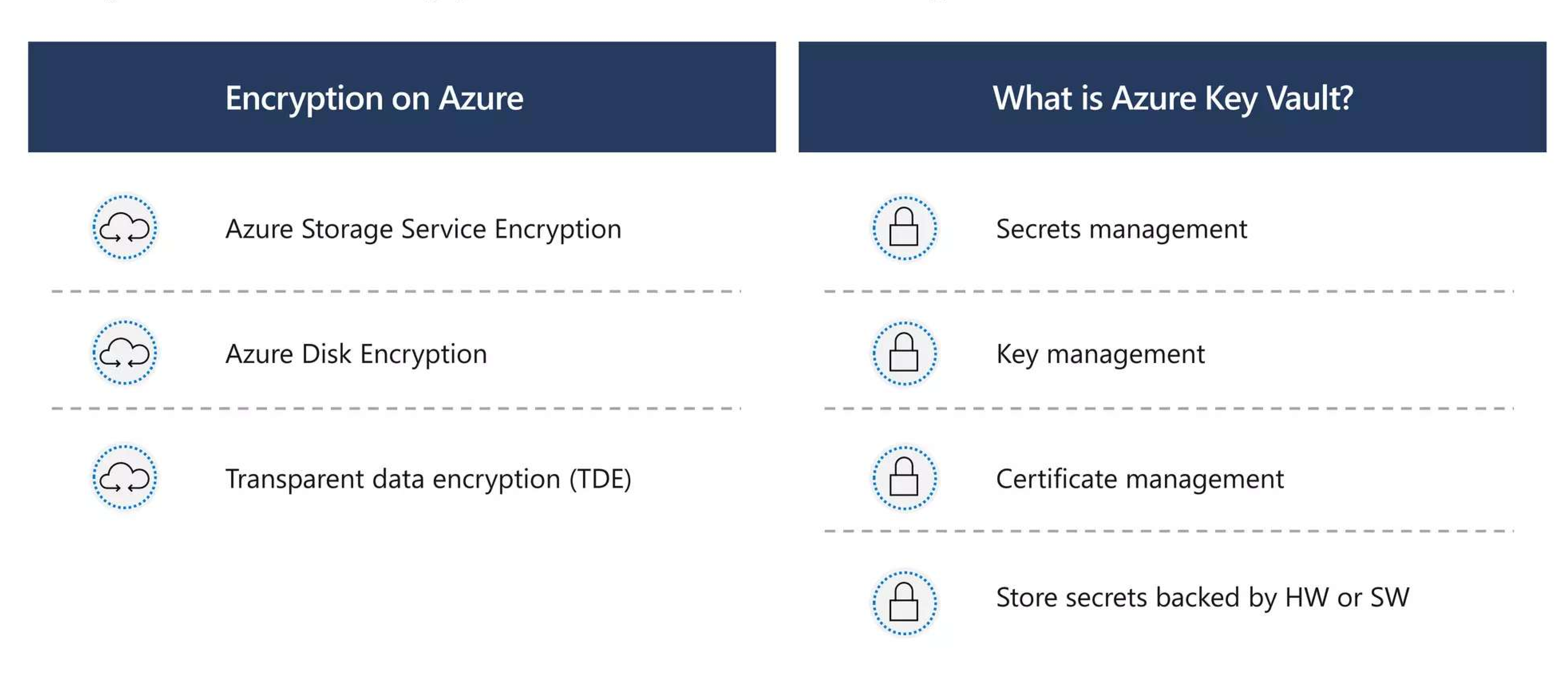
Web Application Firewall

Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities.

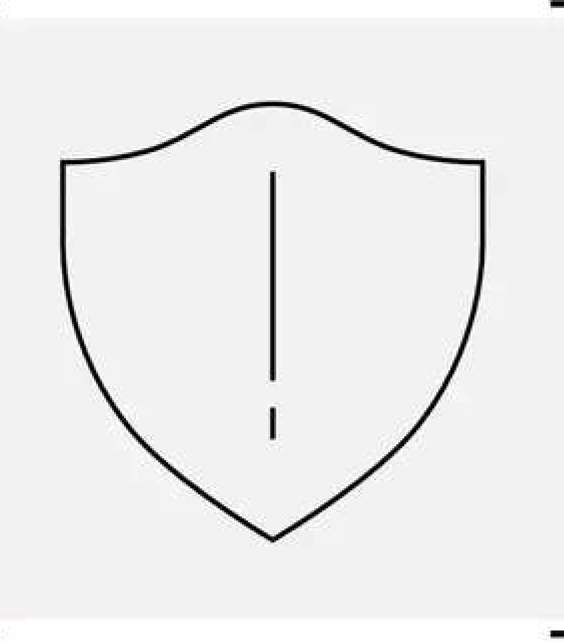
- Simpler security management
- Improves the response time to a security threat
- Patching a known vulnerability in one place
- Protection against threats and intrusions.



Ways Azure encrypts data & use of Key Vault

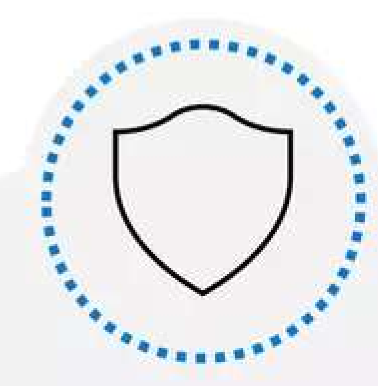


Lesson 2: Describe security management capabilities of Azure



Lesson 2 Introduction

After completing this module, you'll be able to:



Describe the security management capabilities of Azure.



Describe the benefits and use cases of Azure Defender.



Understand Cloud Security Posture Management and the security baseline.

Azure Security Center

Azure Security Center - A unified infrastructure security management system that strengthens the security posture of your data centers and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on premises. Azure Security Center’s features cover two broad pillars of cloud security:



Cloud security posture management(CSPM):

- CSPM uses a combination of tools & services to strengthen your hybrid cloud posture and track compliance with the built-in policies.
- Features include secure score, detection of security misconfigurations in your Azure machines, asset inventory, and more.



Cloud workload protection (CWP):

- Security Center's integrated cloud workload protection platform (CWPP), **Azure Defender**, brings advanced, intelligent, protection of your Azure, non-Azure, and hybrid resources and workloads.
- Defender plans include Azure Defender for servers, App Service, SQL, Key Vault, and more…

Azure Secure Score

The secure score is shown in the Azure portal pages as a percentage value. To improve your secure score, remediate security recommendations from your recommendations list.



Recommendation	Potential increase	Resources
Apply system updates	+ 2% (1 point)	8 of 50 resources
Monitoring agent health issues should be resolved on your machines	Potential increase: 0.96 Current score: 5.04 Max score: 6	4 of 39 virtual machines
Monitoring agent should be installed on virtual machine scale sets (Quick Fix!)		2 of 5 virtual machine scale sets
System updates should be installed on your machines		1 of 39 VMs & servers
Your machines should be restarted to apply system updates		1 of 39 VMs & servers
System updates on virtual machine scale sets should be installed		1 of 5 virtual machine scale sets
Install monitoring agent on your virtual machines (Completed) (Quick Fix!)		None
OS version should be updated for your cloud service roles (Completed)		None
Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version ...		None



Demo

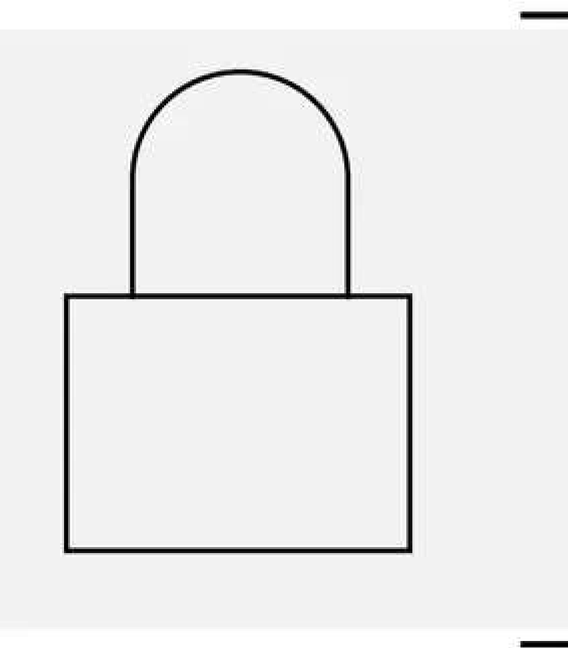
Azure Security Center

Security baselines & the Azure Security Benchmark

Security baselines for Azure offer a consistent experience when securing your environment. They apply prescriptive best practices and recommendations from the Azure Security Benchmark (ASB) to improve the security of workloads, data, and services on Azure. The ASB comprises the security recommendations specific to the Azure platform. Example security baselines include:

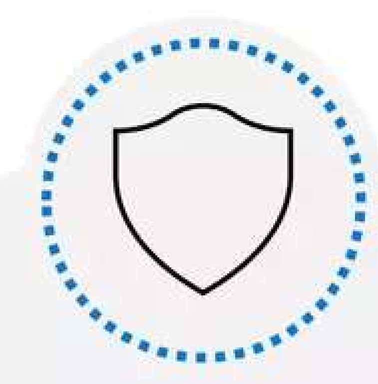


Lesson 3: Describe security capabilities of Azure Sentinel



Lesson 3 Introduction

After completing this module, you'll be able to:



Describe the security concepts for SIEM, SOAR, and XDR.



Describe how Azure Sentinel provides integrated threat protection.



Describe the capabilities of Azure Sentinel.

SIEM, SOAR, and XDR



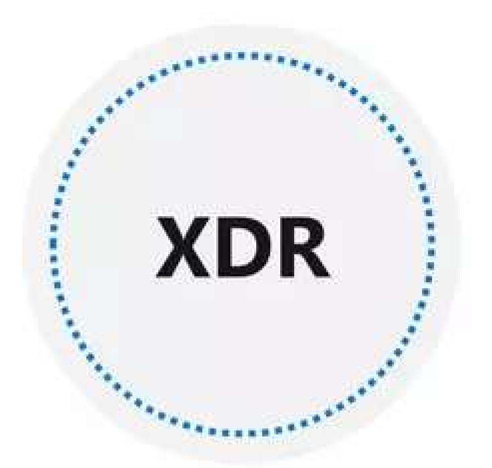
What is security incident and event management?

A SIEM system is a tool that an organization uses to collect data from across the whole estate, including infrastructure, software, and resources. It does analysis, looks for correlations or anomalies, and generates alerts and incidents.



What is security orchestration automated response?

A SOAR system takes alerts from many sources, such as a SIEM system. The SOAR system then triggers action-driven automated workflows and processes to run security tasks that mitigate the issue.



What is extended detection and response?

An XDR system is designed to deliver intelligent, automated, and integrated security across an organization's domain. It helps prevent, detect, and respond to threats across identities, endpoints, applications, email, IoT, infrastructure, and cloud platforms.

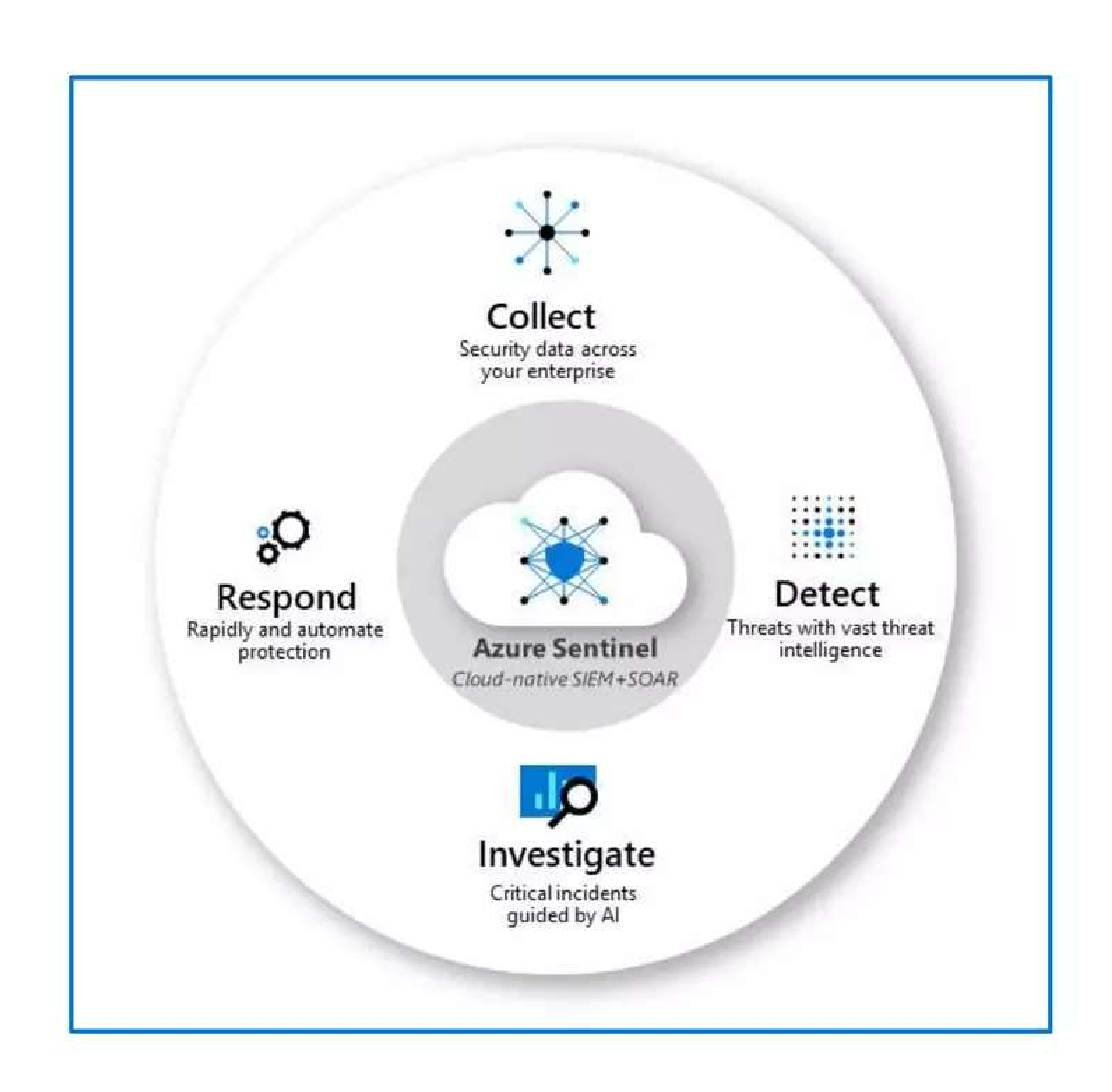
Sentinel provides integrated threat protection (Slide 1)

Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.

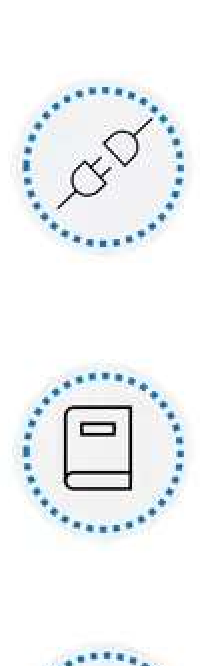
Detect previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence.

Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.

Respond to incidents rapidly with built-in orchestration and automation of common security.



Sentinel provides integrated threat protection (Slide 2)



Connect Sentinel to your data: use connectors for Microsoft solutions providing real-time integration.

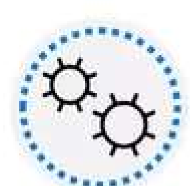
Workbooks: monitor the data using the Azure Sentinel integration with Azure Monitor Workbooks.



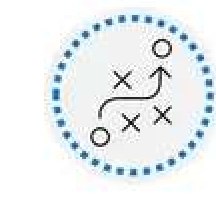
Analytics: Using built-in analytics alerts, you'll get notified when anything suspicious occurs.



Manage incidents: An incident is created when an alert that you've enabled is triggered.



Security automation and orchestration: Integrate with Azure Logic Apps, to create workflows



Playbooks: A collection of procedures that can help automate and orchestrate your response.



Investigation: Understand the scope of a potential security threat and find the root cause.

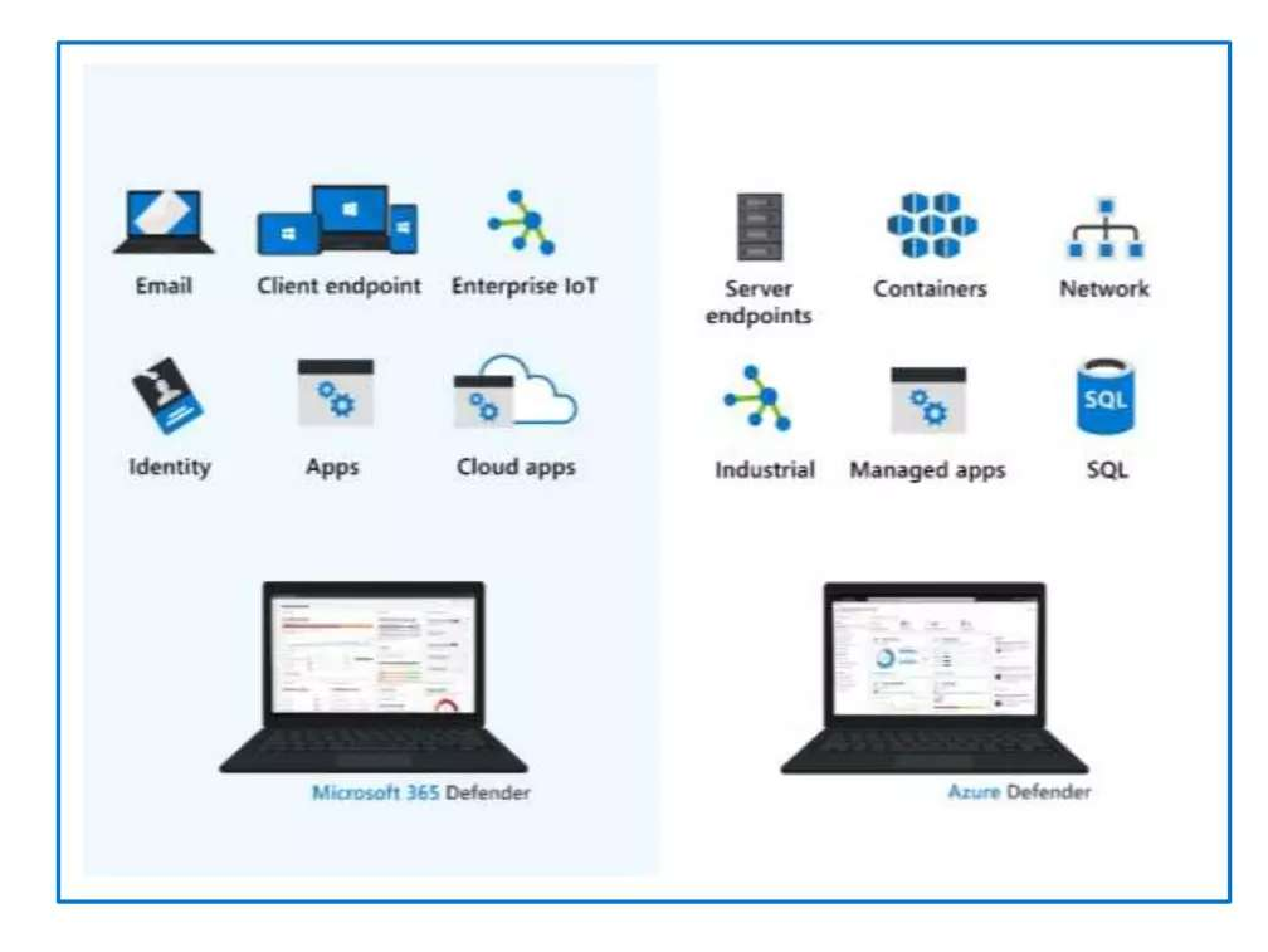


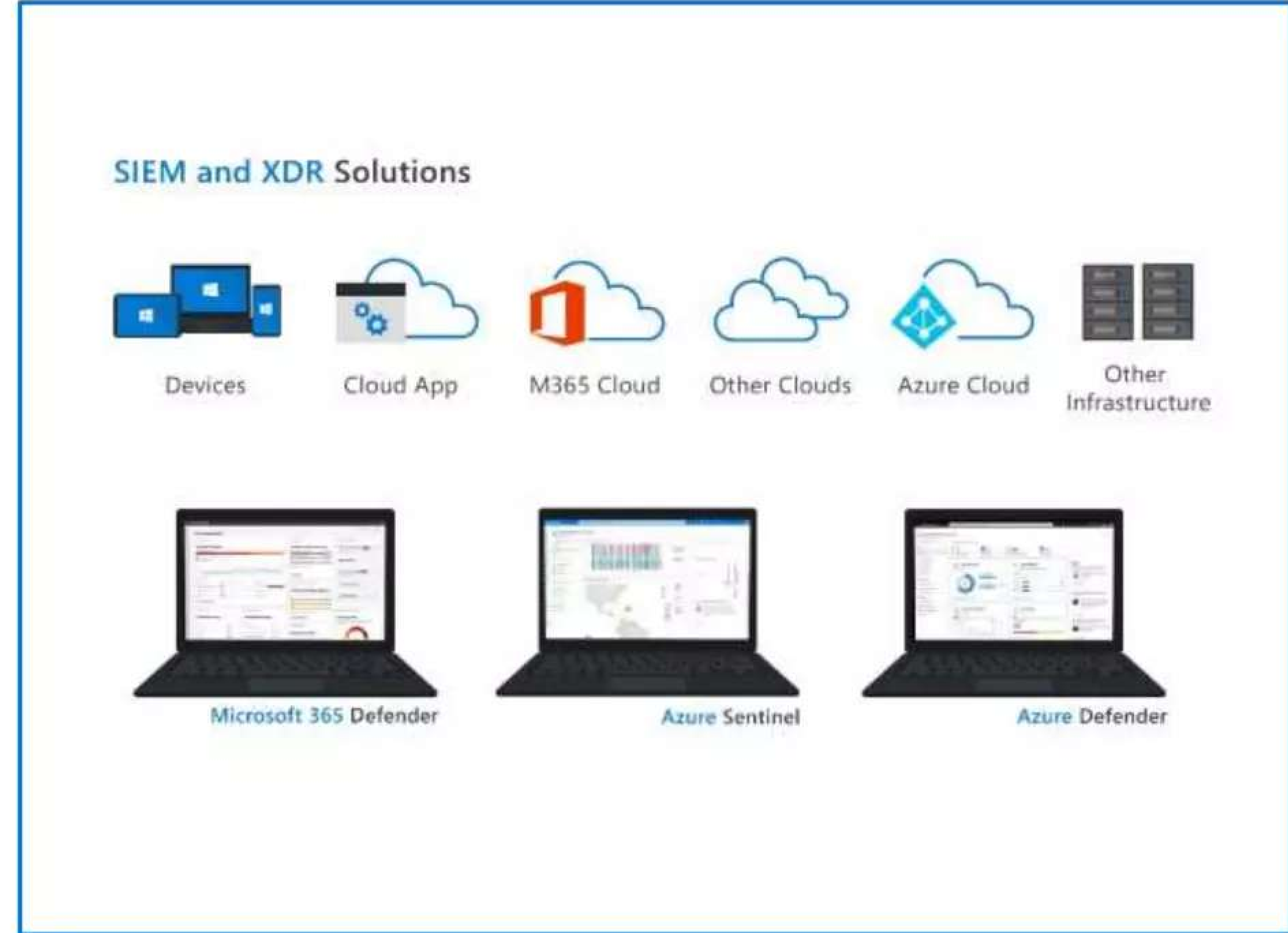
Hunting: Use search-and-query tools, to hunt proactively for threats, before an alert is triggered.



Integrated threat protection: XDR with Microsoft 365 Defender and Azure Defender integration.

Sentinel provides integrated threat protection (Slide 3)



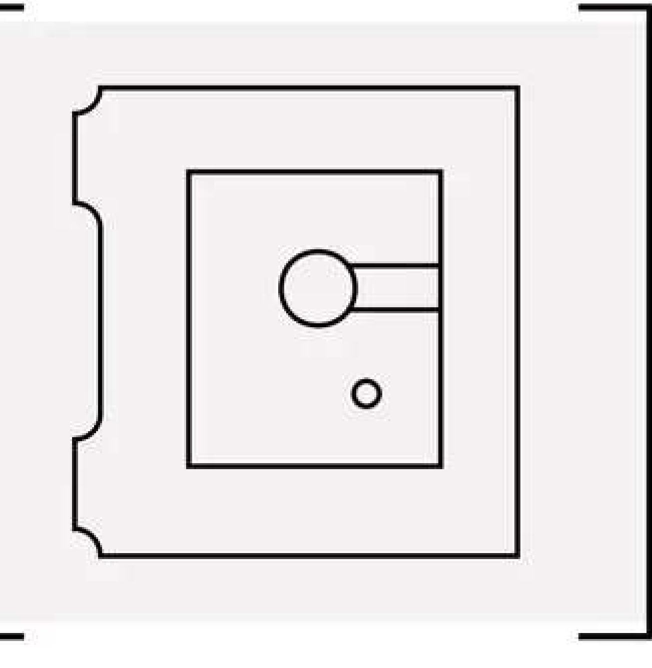




Demo

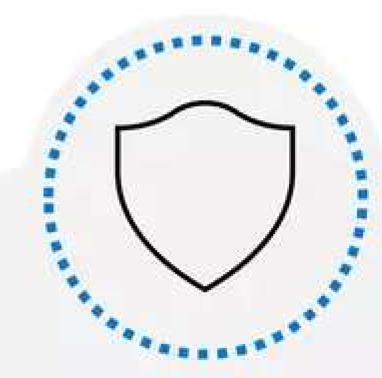
Azure Sentinel

Lesson 4: Describe threat protection with Microsoft 365 Defender



Lesson 4 Introduction

At the end of this module, you'll be able to:



Describe the Microsoft 365 Defender service.



Describe how Microsoft 365 Defender provides integrated protection against sophisticated attacks.



Describe how Microsoft Cloud App Security can help defend your data and assets.

Microsoft 365 Defender services

Microsoft 365 Defender



Natively coordinate the detection, prevention, investigation, and response to threats.



Protects identities, endpoints, apps and email & collaboration.

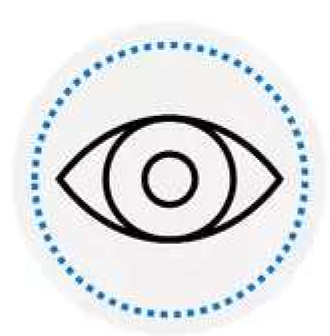
Integrated Microsoft 365 Defender experience

Identity + **Endpoints** + **Apps** + **Email/Collaboration**

Identity	Endpoints	Apps	Email/Collaboration
Microsoft Defender for Identity	Microsoft Defender for Endpoint	Microsoft Cloud App Security	Microsoft Defender for Office 365

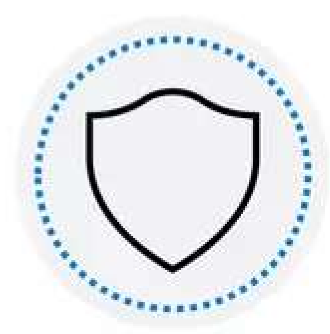
Microsoft Defender for Identity

Microsoft Defender for Identity covers following key areas



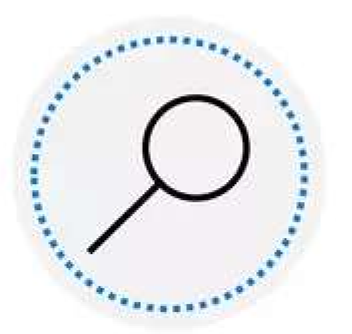
Monitor and profile user behavior and activities

Defender for Identity monitors and analyzes user activities and information across your network, including permissions and group membership, creating a behavioral baseline for each user.



Protect user identities and reduce the attack surface

Defender for Identity gives invaluable insights on identity configurations and suggested security best practices. Through security reports and user profile analytics.



Identify suspicious activities and advanced attacks across the cyberattack kill-chain

- Reconnaissance
- Compromised credentials
- Lateral movements
- Domain dominance



Investigate alerts and user activities

Defender for Identity is designed to reduce general alert noise, providing only relevant, important security alerts in a simple, real-time organizational attack timeline.

Microsoft Defender for Office 365

Microsoft Defender for Office 365 covers:



Threat protection policies



Reports



Threat investigation and response capabilities



Automated investigation and response capabilities

Microsoft Defender for **Office 365 Plan 1**

- Safe Attachments
- Safe Links
- Safe Attachments for SharePoint, OneDrive, & Microsoft Teams
- Anti-phishing protection
- Real-time detections

Microsoft Defender for **Office 365 Plan 2**

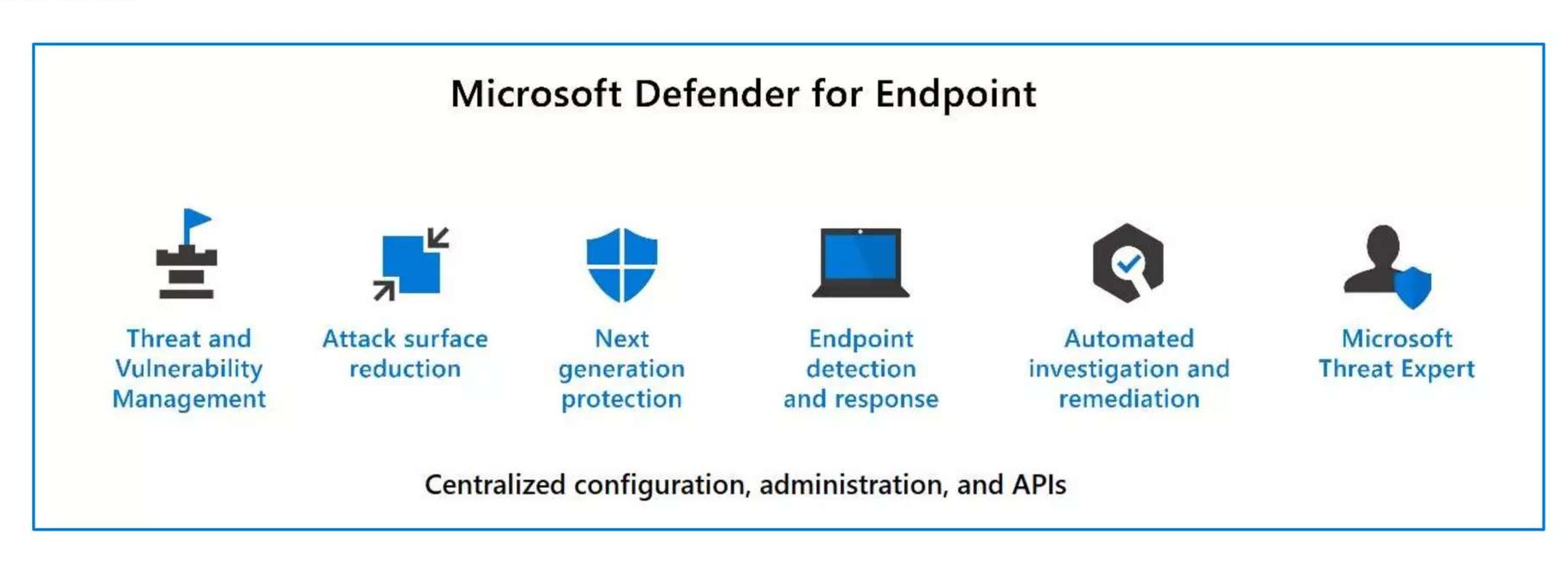
- Threat Trackers
- Threat Explorer
- Automated investigation & response (AIR)
- Attack Simulator

Microsoft Defender for **Office 365 availability**

- Microsoft 365 E5
- Office 365 E5
- Office 365 A5
- Microsoft 365 Business Premium

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is a platform designed to help enterprise networks protect endpoints.



Microsoft Cloud App Security

Microsoft Cloud App Security provides rich visibility to your cloud services, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services.

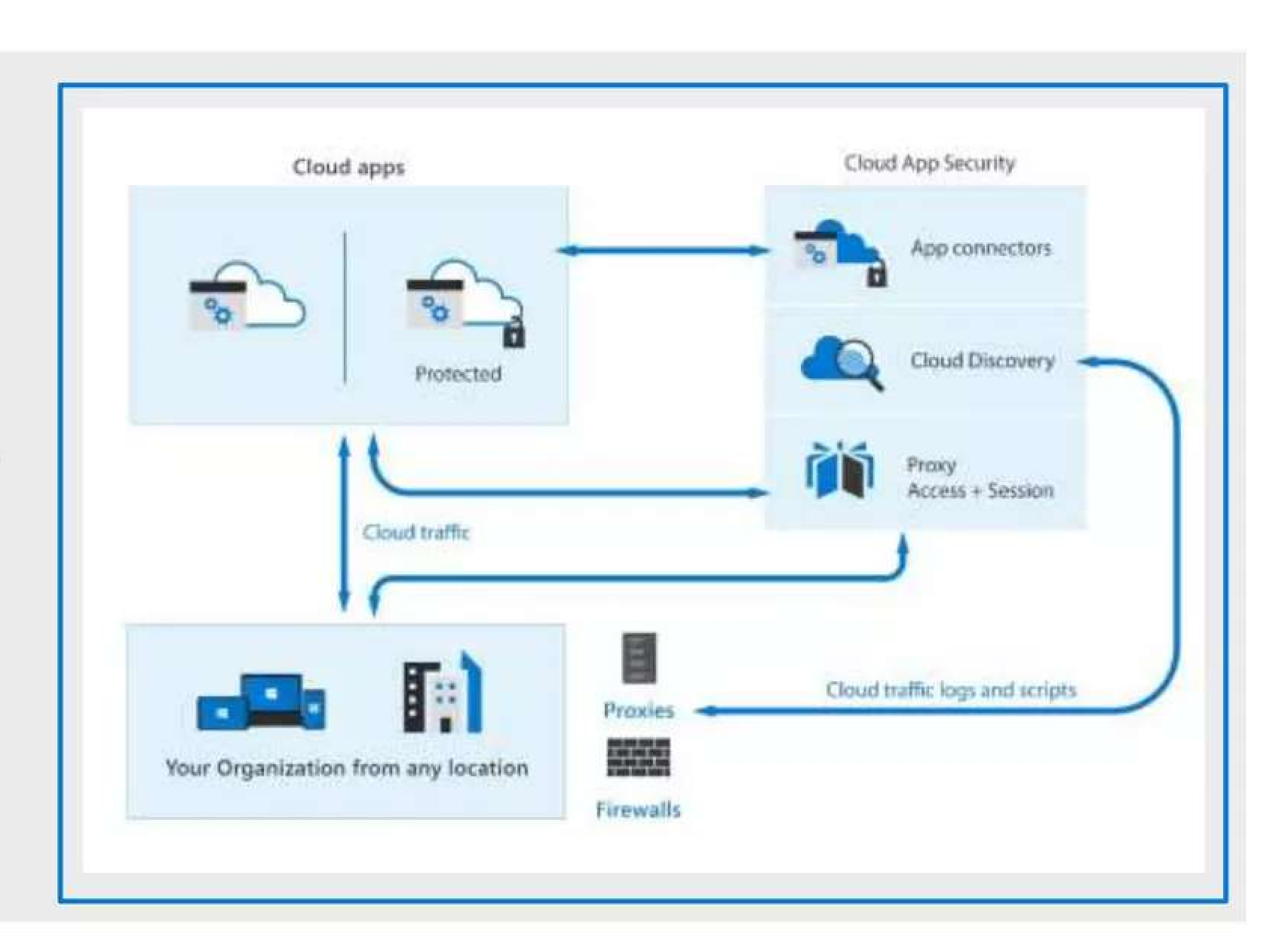
The Cloud App Security framework

- Discover and control the use of Shadow IT
- Protect your sensitive information anywhere in the cloud
- Protect against cyberthreats and anomalies
- Assess your cloud apps' compliance

Office 365 Cloud App Security

Enhanced Cloud App Discovery in Azure Active Directory

Microsoft Cloud App Security architecture

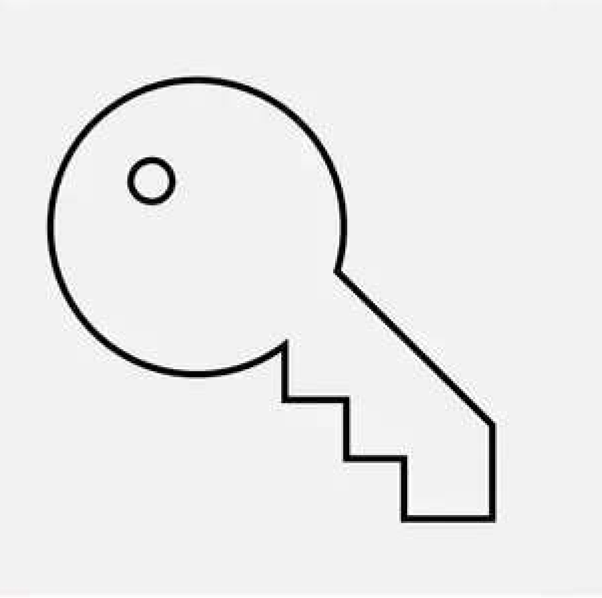




Demo

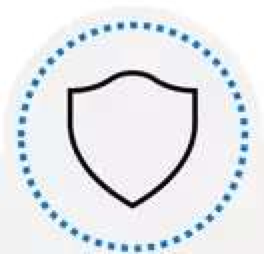
Microsoft Cloud App Security (MCAS)

Lesson 5: Describe security management capabilities of Microsoft 365

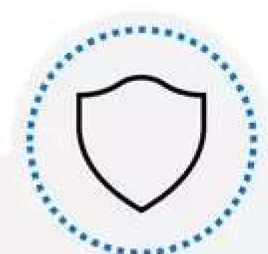


Lesson 5 Introduction

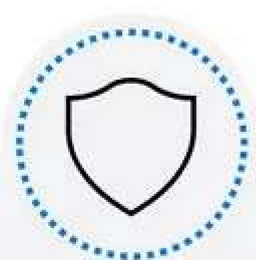
In this module, you will:



Describe and explore the Microsoft 365 Defender portal



Describe how to use Microsoft Secure Score.



Explore security reports and dashboards.



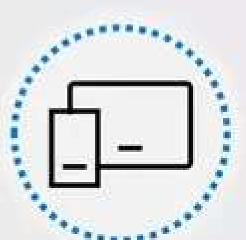
Describe incidents and incident management capabilities.

Microsoft 365 Defender portal

The Microsoft 365 Defender portal combines protection, detection, investigation, and response to email, collaboration, identity, and device threats, in a central portal.



View the security health of your organization.



Act to configure devices, users, and apps.



Get alerts for suspicious activity.

The Microsoft 365 Defender navigation pane include these options and more:



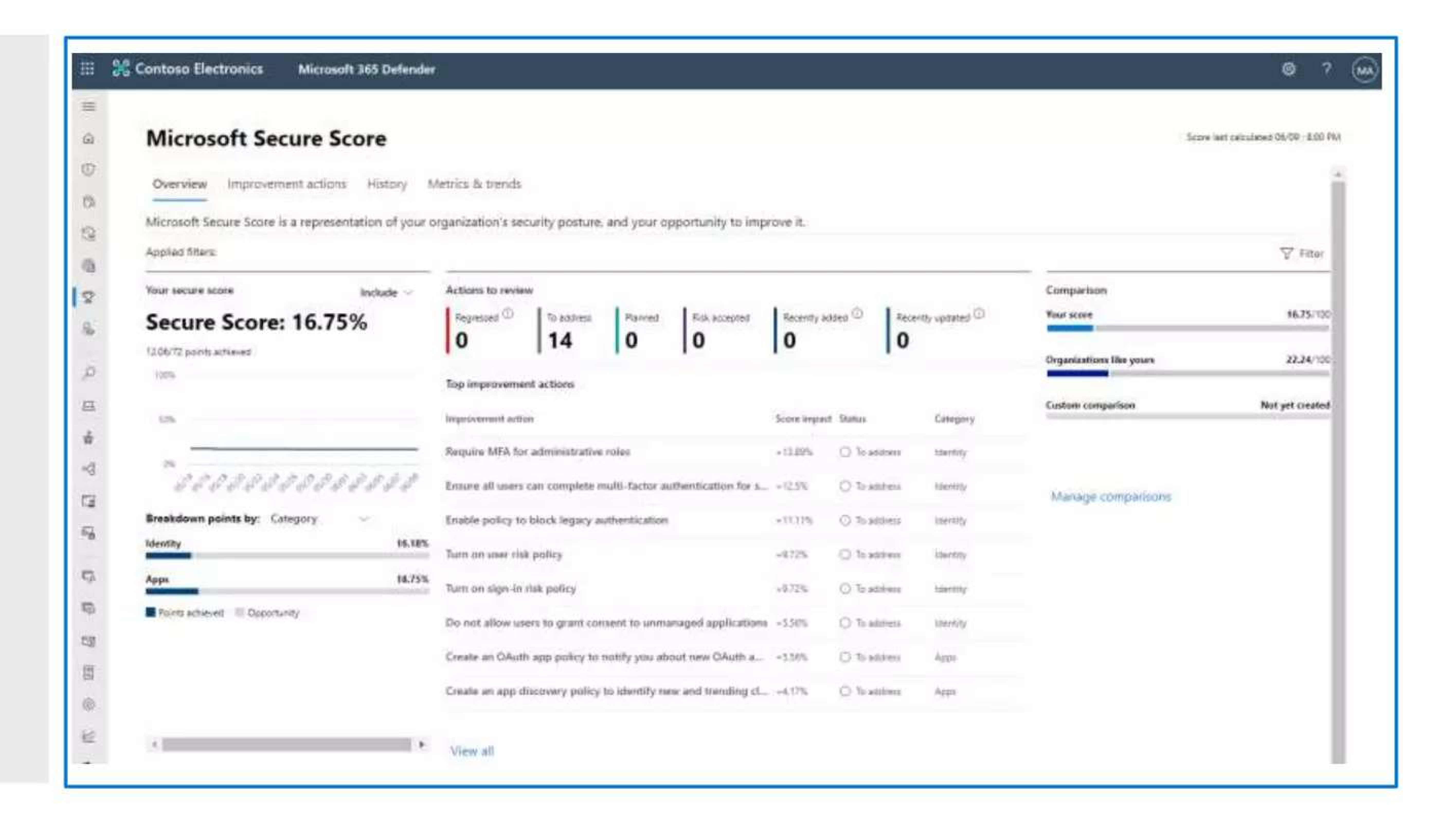
Describe how to use Microsoft Secure Score

Microsoft Secure Score is a representation of a company's security posture.

Will show all possible improvements for the product, whatever the license edition, subscription, or plan.

Supports recommendations for:

- Microsoft 365
- Azure Active Directory
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Cloud App Security





Demo

The Microsoft 365 Defender portal

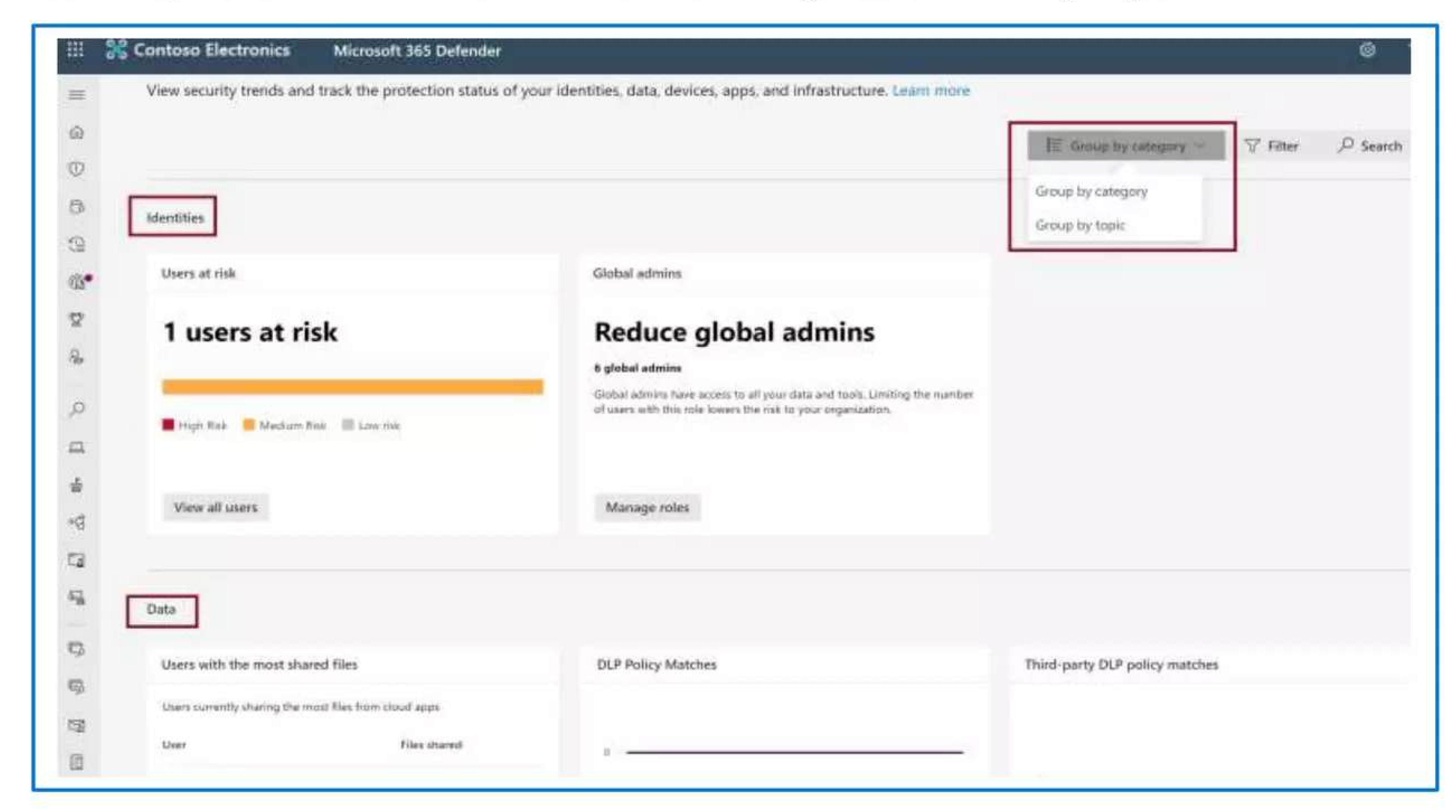
Security reports and dashboards

The Microsoft 365 Defender portal includes a **Reports** section. Shown below is the general security report.

By default, cards are grouped by the following categories:

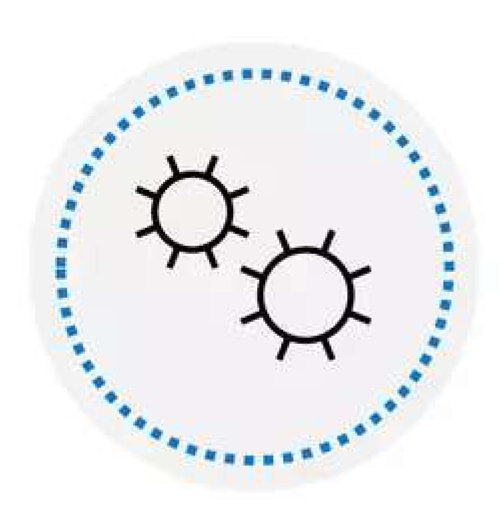
- **Identities** - user accounts and credentials.
- **Data** - email and document contents.
- **Devices** - computers, mobile phones, and other devices.
- **Apps** - programs and attached online services.

You can group cards by topic (risk, detection trends, configuration and health, and other.



Incidents & incident management

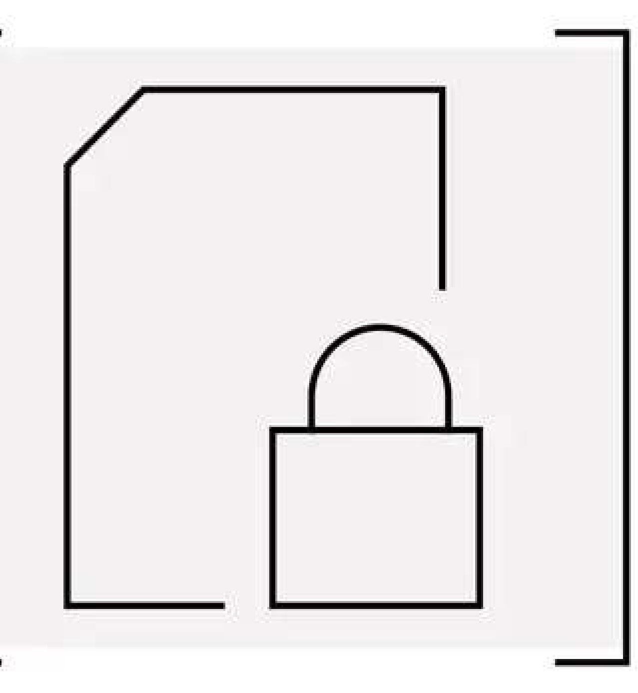
Incidents are a collection of correlated alerts created when a suspicious event is found and provides a comprehensive view and context of an attack.



Incident management

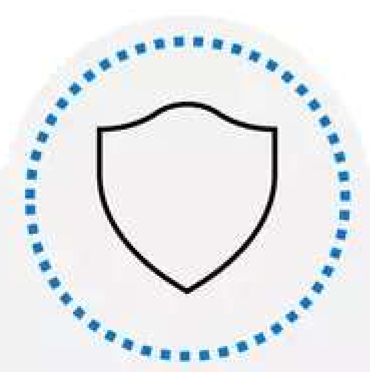
Managing incidents is critical in ensuring that threats are contained and addressed. In Microsoft 365 Defender, you can manage incidents on devices, users accounts, and mailboxes.

Lesson 6: Describe endpoint security with Microsoft Intune

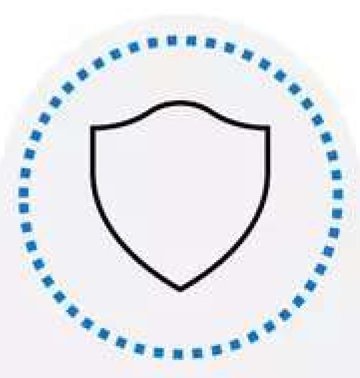


Lesson 6 Introduction

After completing this module, you should be able to:



Describe what Intune is.



Describe the tools available with Intune.



Describe how to manage devices with Microsoft Endpoint Manager.

Intune

Microsoft Intune is a cloud-based service that focuses on **mobile device management (MDM)** and **mobile application management (MAM)**.





When devices are enrolled and managed in Intune, administrators can:

- See the devices enrolled and get an inventory of the ones accessing organization resources.
- Configure devices so they meet your security and health standards.
- Push certificates to devices so users can easily access your Wi-Fi network, or use a VPN to connect to it.
- See reports on users and devices to determine if they're compliant.
- Remove organization data if a device is lost, stolen, or not used anymore.



When apps are managed in Intune, administrators can:

- Add and assign mobile apps to user groups and devices.
- Configure apps to start or run with specific settings enabled and update existing apps already on the device.
- • See reports on which apps are used and track their usage.
- Do a selective wipe by removing only organization data from apps.

Endpoint security with Intune

Manage devices

Manage security baselines

Use policies to manage device security

Use device compliance policy

Role-based access control with Microsoft Intune

Configure conditional access

- Device-based conditional access, to ensure only managed and compliant devices can access network resources.
- App-based conditional access to manage access to network resources by users on devices that aren't managed with Intune.

Integration with Microsoft Defender for Endpoint

- Android
- iOS/iPadOS
- Windows 10 or later



Demo

Microsoft Intune

Module Summary

In this module, you have:

- Learned about threat protection with Microsoft 365 Defender and its component solutions: Microsoft Defender for Identity, Microsoft Defender for Endpoints, MCAS, and Microsoft Defender for Office 365.
- Learned about the security management capabilities of Microsoft 365 with the Microsoft 365 Defender portal and Secure Score.
- Learned about Microsoft Intune.


Microsoft Security